

Guerra de Informação

Saindo de uma abordagem mais voltada para o campo tático, realizada na primeira seção deste número, os três artigos desta seção enveredam por um caminho mais amplo e especulativo, focalizando a disputa pelo domínio das informações no seu aspecto mais elevado, que convencionou-se denominar de Guerra de Informação. As Forças Armadas dos EUA, já há algum tempo, vêm atribuindo um destaque especial a este tema, partindo-se do princípio que o fator fundamental para o sucesso das ações militares futuras reside na obtenção da vitória nesse campo particular da Guerra de Informação. Coerente com essa linha de pensamento, o primeiro artigo analisa o assunto sob o seu aspecto estratégico, enquanto que o segundo procura apontar exageros nessa abordagem fatalística. A seção se completa com a tradução de um artigo recentemente publicado na revista Parameters, o qual analisa os impactos da tecnologia da informação na teoria militar, fazendo um paralelo com ocorrências anteriores, em que revoluções tecnológicas marcantes influenciaram formulações teóricas de pensadores militares.

Guerra de Informação Estratégica: A Nova Face da Guerra

Roger C. Molander, Almirante R/1 Andrew S. Riddile, Marinha dos EUA, e
Peter A. Wilson

Traduzido da revista *Parameters*, Autumn 1996
Copyright 1996

Vivemos em uma era comandada pela informação. Descobertas tecnológicas... estão mudando a face da guerra e a maneira como nos preparamos para enfrentá-la.

—William Perry, Secretário da Defesa

A GUERRA de Informação representa um campo ainda impreciso, mas em rápida evolução, de grande interesse para os planejadores de defesa e formuladores de política. A fonte desse interesse e da imprecisão neste campo é a chamada revolução da informação — liderada pela rápida e contínua evolução do ciberespaço, microcomputadores e tecnologias afins. O organismo de defesa dos EUA, como a sociedade norte-americana em geral, estão agindo rapidamente no sentido de tirar vantagens das novas oportunidades oferecidas por essas mudanças. Adversários atuais e em potencial (e seus aliados) procuram, ao mesmo tempo, a forma de explorar, para fins militares, a infra-estrutura de informação global, em evolução, e as tecnologias associadas.

Próprios de um tema novo e dinâmico, as implicações e os resultados finais dessas contínuas mudanças, para os conflitos internacionais e outras formas de conflito, são extremamente incertos. Será a guerra de informação uma nova, porém subordinada, face da guerra na qual os EUA e seus aliados poderão rapidamente superar suas potências vulnerabilidades no ciberespaço a fim de obter e manter, sejam quais forem, as vantagens militares estratégicas e táticas que possam estar disponíveis nessa arena? Ou serão as mudanças no conflito, moldadas pela revolução da informação, tão rápidas e profundas que resultem numa nova e grave ameaça às tradicionais operações militares e à sociedade norte-americana, mudando fundamentalmente o futuro caráter da guerra?

Em janeiro de 1995, o Secretário da Defesa formou uma Junta Executiva de Guerra de Informação para responder a esta situação e esclarecer incertezas visando auxiliar “o desenvolvimento e a concretização de objetivos de guerra de

informação nacional”. A Corporação RAND foi convocada para apoiar este esforço e fornecer e executar um processo analítico que identificasse os temas-chave da guerra de informação, estudando suas conseqüências e destacando os pontos iniciais relativos ao desenvolvimento de uma política sobre o tema — procurando auxiliar no desenvolvimento de um consenso nacional sustentado para uma estratégia geral de guerra de informação para os EUA.

Para alcançar este objetivo, a Corporação RAND conduziu exercícios baseados em planos e análises do que passamos a chamar o “problema da guerra de informação estratégica”. Esses exercícios, onde participaram os membros mais antigos da comunidade de segurança nacional, bem como representantes das indústrias de sistemas de informações e comunicações relacionados à segurança nacional, guiaram os participantes através de uma hipotética crise de guerra de informação envolvendo uma contingência político-militar regional de grande importância. A metodologia do exercício, conhecida pelo nome “O dia seguinte...”, tinha sido empregada previamente numa variedade de estudos de proliferação nuclear, contraproliferação e de inteligência associada. O cenário específico escolhido para o exercício baseava-se num conflito no fim do século entre o Irã e os Estados Unidos e seus aliados, focalizando uma ameaça à Arábia Saudita.

O exercício foi repetido seis vezes no decurso de cinco meses, de janeiro a junho de 1995, em versões melhoradas. Cada repetição permitia um refinamento dos conceitos estratégicos básicos da guerra de informação e providenciava conhecimentos mais profundos sobre suas implicações de segurança nacional. Este processo oferecia oportunidade de avaliar e analisar as perspectivas dos representantes mais antigos do governo e da indústria em relação a assuntos como, a plausibilidade de cenários de guerra de informações estratégica como o apresentado, possíveis evoluções das ameaças e vulnerabilidades pertinentes com seus desdobramentos nos campos político e



Figura 1. Guerra de Informação Estratégica

estratégico. Proporcionava, também, a oportunidade de identificar escolas emergentes de pensamento e, em alguns casos, um consenso rudimentar sobre os próximos passos a seguir em vários temas importantes de guerra de informação estratégica. Além disso, o processo permitiu visualizar uma estrutura multidimensional que poderia aguçar, em um futuro próximo, o enfoque dos planejadores no desenvolvimento de uma política, de uma estrutura e de objetivos de guerra de informação estratégica, — em particular relacionados às implicações de possíveis contingências regionais sobre estratégias defensivas de guerra de informação, doutrinas, vulnerabilidades e meios. Proporcionou também um foro muito útil para iniciar a coordenação com a indústria sobre a futura direção da estratégia de telecomunicações de segurança nacional relativa à guerra de informação.

Como pôde ser deduzido desde o princípio, a metodologia empregada no estudo parece oferecer vantagens especiais para abordar muitas das dificuldades conceituais inerentes neste assunto. O tema é novo e, em algumas dimensões, tecnicamente complexo, primordialmente para indivíduos que ocupam posições na formulação de políticas. Não se deve subestimar o desafio a ser enfrentado para encontrar técnicas que acelerem eficientemente o desenvolvimento do processo básico de educação nesse assunto e suas implicações para a política e estratégia de segurança nacional.

Este artigo sintetiza os resultados do estudo feito e:

- descreve e formula o conceito de guerra de informação estratégica;
- descreve e discute os aspectos-chave e temas afins que caracterizam a guerra de informação estratégica;
- explora, à medida que surgem no exercício, as consequências dessas características e temas para a segurança nacional dos EUA;
- sugere diretrizes políticas e analíticas para abordar elementos desses temas e aspectos da guerra de informação estratégica.

O que é “Guerra de Informação?”

Dez anos atrás a resposta a essa pergunta dada por um especialista em comunicações, um decodificador, ou qualquer outro membro das comunidades militares ou de inteligência dos EUA poderia ter sido “O quê?”, ou, com um pouco mais de estímulo, “Ah, você que dizer guerra de comando e controle no campo de batalha e no TO, interferência eletrônica e aquela outra coisa de guerra eletrônica”. Hoje em dia, dentro da comunidade de defesa dos EUA, ainda poderia se obter uma resposta não muito diferente das definições anteriores de guerra de comando e controle (*C²W*) ou guerra eletrônica (GE).

Entretanto, em muitos círculos de defesa dos EUA e na ampla comunidade de segurança internacional, o termo guerra de informação está sendo, cada vez mais, usado para abranger um amplo conjunto de conceitos de guerra da era da informação. Esses novos conceitos emergentes da guerra estão diretamente ligados à perspectiva de que a evolução rápida do ciberespaço — a infra-estrutura de informação global — pode trazer tanto novas oportunidades como novas vulnerabilidades. O estudo focaliza uma dessas vulnerabilidades: a perspectiva de que esta revolução possa pôr em risco recursos nacionais de grande valor fora do tradicional campo de batalha e do teatro de projeção de poder de uma forma que afete ambas a estratégia militar nacional e a estratégia mais ampla de segurança nacional dos EUA.

Reconhecemos que, ainda por algum tempo, o termo guerra de informação em linguagem comum não terá mais do que um significado geral, que seja reconhecido por ser inevitavelmente dinâmico. Guerra de informação, da mesma forma que o termo em evolução “guerra estratégica”, se encontra em um estado inicial de desenvolvimento não havendo ainda uma definição aceita do conceito.

Entretanto, pensamos que existe um elemento emergente da guerra de informação — um que parece ser comum a quase todos os empregos deste termo em evolução — que justifica identificação e definição. Classificamos este domínio emergente do conflito, onde as nações usam o ciberespaço para afetar operações militares estratégicas e infligir danos nas infra-estruturas de informação nacional, como guerra de “informação estratégica”. Acreditamos que guerra de informação estratégica, como demonstrado na Figura 1, (em essência a interseção dos conceitos da evolução da guerra de informação e “guerra estratégica” pós-Guerra Fria) justifica uma atenção e reconhecimento especial como uma legítima nova face da guerra com profundas implicações para ambas, a estratégia militar e a estratégia de segurança nacional dos EUA, em geral.¹

Nos últimos anos, a nova cultura e infra-estrutura do ciberespaço mostrada na Figura 1, tem evoluído quase que exclusivamente fora do contexto militar (embora a contribuição da *ARPANET* — *Advanced Research Project*

Agency Network — do Departamento de Defesa para o aparecimento da Internet seja bem conhecida). Como argumentado em outro lugar, os elementos emergentes e as características do ciberespaço por sua natureza oferecem novas oportunidades para a guerra de informação.

Paralelamente, temos a contínua evolução da política internacional, e dentro desse contexto, a inevitável evolução da guerra de Clausewitz como um instrumento da política. Neste ambiente, novos interesses estratégicos estão emergindo para os EUA e outras nações, produzindo novos dilemas e novos (e velhos) alvos estratégicos sobre os quais se deve influenciar — inclusive com a ameaça do emprego de novos (e velhos) tipos de forças estratégicas. Dessa maneira estão emergindo novas ameaças e vulnerabilidades estratégicas. É cada vez mais claro, como este artigo procura mostrar, que a evolução da guerra estratégica incluirá uma dimensão de ameaças e vulnerabilidades no ciberespaço dignas de serem classificadas como “guerra de informação estratégica”.

Guerra de Informação Estratégica

Os EUA contam com um expressivo número de recursos baseados em informação, inclusive sistemas complexos de gerenciamento que abarcam o controle da energia elétrica, do fluxo da moeda, tráfego aéreo, petróleo, gás e outros artigos dependentes da informação. Os aliados e possíveis parceiros de coalizão dos EUA se encontram igualmente dependentes das várias infra-estruturas de informação. Conceitualmente, quando, e se, um adversário em potencial tenta danificar esses sistemas por meio de técnicas de guerra de informação, inevitavelmente esta assume um aspecto estratégico.

O cenário do nosso exercício, desde o princípio, destacou um aspecto fundamental da guerra de informação estratégica: não existe “linha de frente”. Alvos estratégicos nos EUA podem ser tão vulneráveis ao ataque como os alvos de C³I (comando, controle, comunicações e inteligência) no TO. Como resultado, a atenção dos participantes do exercício rapidamente se ampliou além de um único teatro de operações regional para quatro teatros de operações separados como consta na Figura 2: o campo de batalha propriamente dito, “zonas do interior” aliadas (no nosso cenário, o território soberano da Arábia Saudita); a zona intercontinental de comunicações e desdobramento; e a zona do interior dos EUA.

O enfoque do componente regional da estratégia militar nacional dos EUA pós-Guerra Fria descreve, de forma incompleta, este tipo de cenário e sua relevância é pequena em um possível ambiente estratégico internacional futuro. Quando respondendo a ataques de guerra de informação deste tipo, a estratégia militar não pode mais dar-se o luxo de focar a condução e apoio de operações apenas na região de interesse. Hoje em dia é necessário examinar detalhadamente as implicações da guerra de informação



nas infra-estruturas aliadas e dos EUA, que dependem do gerenciamento livre da informação.

Características Básicas da Guerra de Informação Estratégica

Os exercícios destacaram sete características que definem a guerra de informação estratégica:

- *Baixo custo de entrada.* Ao contrário das tecnologias tradicionais de armamentos, o desenvolvimento de técnicas baseadas em informação não requer grandes recursos financeiros ou financiamento do estado. Provavelmente os únicos pré-requisitos sejam o conhecimento dos sistemas de informação e o acesso a redes importantes.
- *Limites tradicionais indefinidos.* Distinções tradicionais — interesse público versus interesse particular, comportamento belicoso versus criminoso — e limites geográficos, tais como aqueles historicamente definidos entre as nações, são mascarados pela interação crescente que existe dentro da infra-estrutura da informação.
- *Maior papel para a administração da percepção.* Novas técnicas baseadas na informação podem substancialmente aumentar o poder de dissimulação e das atividades de manipulação da imagem, dificultando drasticamente os esforços do governo de construir apoio político para iniciativas relativas à segurança.
- *Um novo desafio para a inteligência estratégica.* Quando mal interpretados os alvos e as vulnerabilidades de guerra de informação estratégica reduzem a eficácia dos métodos clássicos de coleta e análise de informações. Teremos, portanto, que desenvolver um novo campo de análise focalizado na guerra de informação estratégica.
- *Dificuldades de alerta tático e problemas de avaliação de ataque.* Não existe atualmente um sistema de alerta adequado que facilite a distinção entre ataques de guerra de informação estratégica e outros tipos de atividades do ciberespaço, incluindo espionagem ou acidentes.
- *Dificuldade de formar e manter coalizões.* A

Em muitos círculos de defesa dos EUA e na ampla comunidade de segurança internacional, o termo guerra de informação está sendo, cada vez mais, usado para abranger um amplo conjunto de conceitos de guerra da era da informação. Esses novos conceitos emergentes da guerra estão diretamente ligados à perspectiva de que a evolução rápida do ciberespaço — a infra-estrutura de informação global — pode trazer tanto novas oportunidades como novas vulnerabilidades. . . . ainda por algum tempo, o termo guerra de informação em linguagem comum não terá mais do que um significado geral, que seja reconhecido por ser inevitavelmente dinâmico. Guerra de informação, da mesma forma que o termo em evolução “guerra estratégica”, se encontra em um estado inicial de desenvolvimento não havendo ainda uma definição aceita do conceito.

confiança depositada nas coalizões irá provavelmente aumentar a vulnerabilidade das posturas de segurança de todos os parceiros aos ataques de guerra de informação estratégica, dando aos oponentes uma grande vantagem estratégica.

● *Vulnerabilidade do território dos EUA.* Técnicas baseadas na informação tornam a distância geográfica irrelevante; alvos nos EUA são tão vulneráveis como os que se encontram no teatro de operações. A grande confiança que a sociedade e a economia norte-americana deposita na infra-estrutura da rede de informações de alto desempenho, converte-se, para os potenciais oponentes armados para guerra de informação, em um novo conjunto de alvos estratégicos lucrativos.

Durante o curso de nosso exercício baseado em análises, formuladores de política e outros peritos dos setores particular e público foram incitados a explorar o caráter e as conseqüências desses aspectos. A discussão a seguir resume as observações feitas pelos participantes do exercício referentes às características e implicações desses aspectos para o problema da guerra de informação estratégica. Observe o efeito “cascata” inerente nessas observações — cada uma ajuda a criar as condições condizentes para as subseqüentes.

Baixo Custo de Entrada

Redes interconectadas estão sujeitas a ataques e interrupções não apenas por estados constituídos, mas também por organizações privadas, inclusive grupos dispersos e

até mesmo indivíduos. Adversários em potenciais também poderiam possuir uma ampla gama de meios. Assim sendo, a ameaça aos interesses dos EUA poderia ser multiplicada substancialmente e continuaria a mudar à medida que sistemas mais complexos fossem produzidos e os conhecimentos exigidos fossem amplamente difundidos.

Alguns participantes acreditavam que o preço de entrada sugerido nos vários tipos de ataques de guerra de informação poderia subir ao ser negado o fácil acesso às redes e sistemas de controle, através da exploração de novas técnicas de criptografia para software. Outros participantes reconheceram que tal fato poderia mitigar algumas ameaças, mas enfatizavam que esta abordagem não removeria outras ameaças feitas a um sistema de rede por um operador corrupto, um ataque físico direto, ou ambos. Também aumentaria a dificuldade de desenvolvimento de inteligência relativa aos adversários na guerra de informação estratégica em todos os níveis: estratégico, operacional e tático.

Limites Tradicionais Indefinidos

A grande variedade de possíveis oponentes, armamentos e estratégias, dificulta, cada vez mais, a distinção entre as fontes doméstica e estrangeira de ações e ameaças de guerra de informação. Provavelmente, não poderemos saber quem está sendo atacado, ou quem está atacando. Esse fato dificulta imensamente a tradicional distinção entre a imposição de uma lei interna, por um lado, e a segurança nacional e as entidades de inteligência por outro. Outra conseqüência deste fenômeno de indefinição é o desaparecimento de identificação clara dos diferentes níveis de atividade anti-estado, que variam desde o crime até a guerra. Em virtude desta indefinição, nações-estado contrárias aos interesses estratégicos dos EUA poderiam abster-se de realizar ações militares ou terroristas tradicionais e, ao invés disso, explorar indivíduos ou organizações criminais transnacionais para conduzir “operações criminosas estratégicas”.

Maior Papel para a Administração da Percepção

Existe a crescente possibilidade de que agentes da guerra de informação manipulem a informação-chave destinada à percepção pública. Por exemplo, grupos políticos e outras agências não governamentais podem usar a Internet para galvanizar o apoio político, como fizeram os Zapatistas em Chiapas, no México. Existe ainda a probabilidade de os “fatos” de um acontecimento serem manipulados e amplamente disseminados pelas técnicas de multimídia. Por outro lado, poderá haver uma reduzida capacidade de construir e manter o apoio doméstico para ações políticas controversas. Outra possibilidade é que as futuras administrações dos EUA incluam um robusto componente da Internet como parte de qualquer campanha de informação pública.

Não havia, entre os participantes, apoio para nenhuma

manobra extraordinária do governo para “retomar o controle” da mídia e da Internet em resposta a um provável ataque da guerra de informação. Pelo contrário, havia um reconhecimento que as futuras administrações norte-americanas teriam de enfrentar a desencorajadora tarefa de organizar e manter o apoio doméstico para as ações marcadas por elevado grau de ambigüidade e incerteza da área da guerra de informação.

Falta de Inteligência Estratégica

Por uma variedade de razões, os métodos de coleta e análise da inteligência tradicionais terão um emprego limitado para satisfazer as necessidades de inteligência da guerra de informação estratégica. Alvos de coleta são de difícil identificação; a alocação de meios de inteligência é problemática devido à natureza mutante da ameaça; e, ainda não há uma boa compreensão das vulnerabilidades e dos alvos. Em suma, os EUA talvez tenham dificuldade de identificar adversários em potencial, suas intenções e suas capacidades. Uma implicação decorrente disso é que novos relacionamentos organizacionais são necessários dentro da comunidade de inteligência, e entre esta comunidade e outras entidades. Também, poderá ser necessária uma reestruturação de papéis e missões.

Durante os exercícios, os debates sobre este problema centravam-se na necessidade de se estabelecer uma certa estrutura interagências, que permitisse uma coleta e análise coordenada de fontes domésticas e externas contra o desejo de preservar o limite entre a inteligência externa e a imposição das leis internas.

Dificuldade de Alerta Tático e Avaliação do Ataque

Esta característica da guerra apresenta fundamentalmente novos problemas num ambiente de ciberespaço. Um problema básico é distinguir entre o ataque e outros acontecimentos, tais como acidentes, panes de sistemas ou ações de *hackers*. A principal conseqüência desta característica é que os EUA talvez não saibam quando um ataque está a caminho, quem está atacando, ou como o ataque está sendo conduzido.

Da mesma forma que no debate a respeito dos dilemas apresentados pelo desafio de inteligência estratégica, os participantes do exercício dividiram-se entre aqueles que estavam preparados para considerar uma mescla mais radical de imposição de leis internas e instituições de inteligência estrangeiras e aqueles que definitivamente se opunham a qualquer mistura.

Dificuldade em Formar e Manter Coalizões

Muitos aliados norte-americanos e parceiros de coalizão estarão vulneráveis a ataques de guerra de informação ao cerne de sua estrutura de informação. Por exemplo, a dependência

em telefones celulares nos países em desenvolvimento bem poderia tornar as comunicações telefônicas, naquelas nações, altamente suscetíveis a interferências. Outros setores podem também apresentar vulnerabilidades durante os estágios iniciais de exploração da revolução de informação (por exemplo: energia e financiamento) que levarão um adversário a atacar com o objetivo de solapar os planos da coalizão. Tais ataques poderiam também ser empregados para romper os “elos fracos” durante a execução dos planos da coalizão. Por outro lado, prováveis parceiros de coalizão que precisam urgentemente de assistência militar podem exigir uma certa garantia dos EUA de que o plano de desdobramento para a sua região não é vulnerável a interrupções da guerra de informação.

Embora houvesse um acordo geral entre os participantes para que à medida que os Estados Unidos desenvolvessem e melhorassem os sistemas de defesa e os conceitos de operações ou técnicas nessa área, ele deveria considerar compartilhá-los com seus aliados-chave, nenhuma política foi oferecida durante esses debates.

Vulnerabilidade do Território dos EUA

Como mencionado anteriormente, a guerra de informação não tem linha de frente. Campos de batalha em potencial se encontram em qualquer lugar onde os sistemas de redes permitem acesso. As tendências atuais sugerem que a economia norte-americana irá, cada vez mais, depender de complexos e interconectados sistemas de controle de redes para instalações como oleodutos, gasodutos e redes de energia elétrica. Atualmente, a vulnerabilidade destes sistemas não é muito bem entendida. Além das ameaças de guerra de informação, os meios de dissuasão e represália são incertos e podem depender de instrumentos militares tradicionais. Em suma, o território norte-americano talvez não mais propicie um santuário contra os ataques externos.

Existia entre os participantes do exercício um amplo consenso de que medidas extremas como a paralisação de uma infra-estrutura pudesse ser eficaz como medida de defesa (e também havia algum ceticismo se esta ação poderia, de fato, ser realizável durante uma crise). Contudo, parecia haver um amplo consenso a favor da exploração do conceito de uma “estrutura de informação essencial mínima”, apoiada numa série de incentivos federais para garantir que os proprietários e operadores tivessem meios de detectar ataques de guerra de informação e medidas de reconstituição que minimizassem os efeitos de interrupção de qualquer rede.

Conclusões — Avaliação Indefinida sobre a Ameaça

No decurso dos exercícios, houve um grande esforço para que se chegasse a uma possível conclusão sobre a gravidade da ameaça de guerra de informação estratégica alicerçada no ciberespaço. Muitos dos sistemas de

Avaliação	Descritor
Não é problema – nem agora, nem nunca.	"Os EUA é a única superpotência sobrevivente."
Problema em potencial: os EUA são superiores em qualquer área.	"Eles não se atreveriam."
Problema em potencial: os EUA são tecnologicamente superiores.	"Eles são muito bobos."
Problema em potencial: os EUA podem empregar força bruta.	"Podemos tolerar."
Problema atual: nenhuma ação é necessária por parte dos EUA.	"A infra-estrutura de informação dos EUA automaticamente se recuperará."
Problema atual: algumas ações são necessárias por parte dos EUA.	"A infra-estrutura de informação dos EUA pode ser recuperada manualmente."
Problema atual e ficando pior.	"Os EUA dependem cada vez mais de sistemas de informações vulneráveis"
Não poderia ser pior.	"Os EUA podem agora ser rapidamente colocados de joelhos por algumas pessoas inteligentes".

Figura 3. Um Amplo Espectro de Perspectivas

informação existentes parecem ser vulneráveis a um certo nível de interrupção ou uso impróprio. Ao mesmo tempo, os progressos em ciberespaço são tão dinâmicos que as vulnerabilidades existentes podem estar aumentadas, como parte da formação natural de imunidades contra ameaças que acompanham a evolução rápida de qualquer entidade. No entanto, nossa dependência no ciberespaço e nos sistemas de informação também está crescendo rapidamente — surgindo perguntas inquietantes sobre a capacidade de se manter o processo de “imunização do sistema” e, conseqüentemente, evitar o surgimento e a exploração de sérias vulnerabilidades estratégicas.

Procuramos e não encontramos qualquer estatística que representasse o pensamento do povo sobre onde nos encontramos agora no espectro de ameaças representado na Figura 3, ou para onde nos encaminhamos. Observamos, contudo, que durante o transcurso do exercício, a perspectiva geral sobre a magnitude do problema da guerra de informação estratégica, na maioria das vezes, parecia mover-se para baixo ao longo da escala da Figura 3. Esta experiência reflete a dos autores — quanto mais tempo gastamos neste assunto, mais problemas sérios encontramos, sem obter uma solução concreta e, em alguns casos, sem ao menos ter uma boa idéia de onde começar.

Os aspectos e possíveis conseqüências da guerra de informação estratégica apontam para uma conclusão básica: as pressuposições básicas da estratégia militar nacional são obsoletas e inadequadas para enfrentar a ameaça imposta pela guerra de informação estratégica. Cinco recomenda-

ções principais emergiram desses exercícios como pontos de partida para abordar este problema:

- *Liderança: Quem deveria ficar com essa missão no Governo?*

Os participantes, em sua maioria, concordaram que o primeiro passo, imediato e de grande necessidade, é determinar um ponto focal na liderança do governo federal para desenvolver uma resposta coordenada dos Estados Unidos contra a ameaça da guerra de informação estratégica. Este ponto focal deve estar localizado no Gabinete Executivo do Presidente, já que somente neste nível é possível realizar eficazmente a necessária coordenação do grande número de organizações governamentais envolvidas neste assunto, bem como realizar as necessárias interações com o Congresso. Este gabinete deveria ser também responsável pela coordenação aproximada com a indústria, uma vez que a infra-estrutura de informação da nação está sendo desenvolvida quase que exclusivamente pelo setor comercial. Com isto estabelecido, essa liderança de alto nível deveria assumir imediatamente a responsabilidade para iniciar e administrar uma revisão completa dos temas de guerra de informação estratégica a nível nacional.

- *Avaliação do Risco*

A entidade de liderança do governo federal, acima mencionada, deveria, como primeiro passo, conduzir imediatamente uma avaliação de risco para determinar, tanto quanto possível, a vulnerabilidade dos elementos-chave das atuais estratégias militar e de segurança nacional com respeito à guerra de informação estratégica. Devem ser objetos dessa revisão o conjunto de alvos estratégicos, os efeitos da guerra de informação, e a avaliação da ameaça e da vulnerabilidade paralela. Num ambiente de mudanças dinâmicas nas ameaças e vulnerabilidades do ciberespaço, não existe uma base estável para uma decisão presidencial em assuntos de guerra de informação estratégica, sem a avaliação de riscos.

Neste contexto existe sempre a esperança ou a crença — vimos as duas durante os exercícios — que o tipo de resposta agressiva sugerida neste relatório pode ser protelada enquanto o ciberespaço tiver chances de incrementar suas próprias defesas. De fato, isso é uma possibilidade. O restabelecimento e o fortalecimento de um sistema imune, que está, e certamente continuará a estar, sob constante assalto, como é o caso do ciberespaço (segundo as palavras de Willy Sutton, porque é aí onde se encontra o dinheiro), irá criar a robusta infra-estrutura de informação nacional que todos esperam utilizar. Mas, isso pode não acontecer. E, sem dúvida, ainda não chegamos lá.

- *Papel do Governo*

O papel do governo em sua resposta à ameaça de guerra de informação estratégica precisa ser abordado, reconhecendo-se que esse papel — será, sem dúvida, metade por sua própria liderança e metade por parceria com o setor doméstico — irá certamente evoluir. O governo obviamente já realiza certas funções de preparação básica, como

organização, equipamento, adestramento e manutenção das forças militares. Além disso, ele pode ter um papel mais produtivo e eficaz como facilitador e mantenedor de alguns sistemas e da infra-estrutura de informação. Pode, também, por meio de mecanismos políticos abater impostos, estimular a redução das vulnerabilidades e melhorar a capacidade de recuperação e reconstituição.

Um fator importante é a tradicional mudança no papel do governo à medida que passa da defesa nacional, através da segurança pública, em direção a situações que representam o que é melhor para o povo. Sem dúvida, o papel do governo, como é percebido nesta área, terá que ser equilibrado entre as percepções do povo sobre a perda de liberdades civis e a preocupação do setor comercial sobre limites injustificados nas suas práticas e nos seus mercados.

● *Estratégia de Segurança Nacional*

Uma vez completada a avaliação inicial dos riscos, a estratégia de segurança nacional dos EUA precisa abordar a preparação para enfrentar a ameaça que foi identificada. A preparação atravessará vários limites tradicionais, do militar para o civil, do exterior para o doméstico, e do nacional para o local.

Um meio promissor para instituir este tipo de preparação poderia envolver o conceito de “infra-estrutura de informação essencial mínima” (IIEM), o qual foi introduzido como uma possível iniciativa de guerra de informação defensiva estratégica. O IIEM é concebido como o conjunto mínimo de sistemas de informações dos Estados Unidos, procedimentos, leis, e incentivos fiscais necessários, para garantir a continuação do funcionamento da nação, mesmo face a um sofisticado ataque de guerra de informação estratégica. Uma faceta do IIEM poderá ser um conjunto de regras e regulamentos emitidos pelo governo federal para incentivar proprietários e operadores das várias infra-estruturas nacionais a tomarem medidas para reduzir a vulnerabilidade daquelas infra-estruturas, garantir rápida reconstituição em caso de ataques de guerra de informação, ou ambos. Uma concepção análoga a esta é a Rede de Comunicações de Emergência Essencial Mínima — RCEEM (*Minimum Essential Emergency Communications Network - MEECN*) da estratégia nuclear. Os participantes do exercício julgaram o modelo IIEM

conceitualmente muito bom, embora houvesse alguma incerteza sobre sua implementação. Uma avaliação sobre exequibilidade de um IIEM (ou conceitos similares) deveria ser realizada com antecedência.

● *Estratégia Militar Nacional*

A presente estratégia militar nacional enfatiza a manutenção da capacidade de projeção de poder dos EUA nos teatros de operações em regiões-chave da Europa e da Ásia. Devido aos quatro teatros de operações emergentes no ciberespaço para este tipo de contingência (ver Figura 2), a guerra de informação estratégica reduz drasticamente a importância da distância em relação ao desdobramento e emprego de armamentos. Portanto, as vulnerabilidades de C³I no campo de batalha podem tornar-se menos significativas do que as vulnerabilidades da infra-estrutura nacional. Planejar pressuposições fundamentais com base na atual estratégia militar nacional é um método obsoleto. As considerações características de guerra de informação devem ser incluídas na estratégia militar nacional norte-americana.

Contra esta difícil situação de projeção e avaliação, existe o sempre presente risco de que os Estados Unidos possam se envolver em uma crise a curto prazo, enfrentando a possibilidade de um ataque de guerra de informação estratégica. Quando o Presidente perguntar se os EUA estão sob um ataque típico de uma guerra de informação — em caso de uma resposta afirmativa, quem é o atacante, e se o plano e as estratégias das FA são vulneráveis — um simples “não sabemos” não será uma resposta aceitável. Finalmente, deve-se reconhecer que guerra de informação estratégica é um conceito muito recente que apresenta uma nova coleção de problemas. Estes problemas podem muito bem ter uma solução — mas não sem um emprego inteligente e adequado de energia, liderança, dinheiro, e outros recursos escassos, para o qual esperamos que este artigo seja um catalisador. **MR**

REFERÊNCIAS

1. Ver nosso relatório mais detalhado, também intitulado *Strategic Information Warfare: A New Face of War* (Santa Mônica, Califórnia: RAND, 1996). O presente artigo foi baseado no Sumário e no Capítulo 1. O texto completo de estudo encontra-se no site da RAND no World Wide Web. O endereço URL é: <http://www.rand.org/publications/MR/MR661/MR661.pdf>

Roger C. Molander é pesquisador sênior na Corporação RAND, especializando-se em guerra de informação e proliferação nuclear. O Dr. Molander trabalhou como assessor do Conselho Nacional de Segurança da Casa Branca, foi presidente do Roosevelt Center for American Policy Studies, e foi também diretor executivo do Ground Zero, projeto de educação sobre guerra nuclear, não filiado a nenhum partido político, voltado para o público norte-americano e a mídia. Foi co-autor do livro The Day After... Study: Nuclear Proliferation in the Post-Cold War World.

Almirante R/1 Andrew S. Riddle (Reserva da Marinha dos EUA) é consultor da Corporação RAND trabalhando na área de pesquisa de segurança nacional.

Peter A. Wilson é consultor da Corporação RAND e do Instituto Washington. Trabalhou anteriormente no Instituto para Análises de Defesa, SAIC, CIA, no Departamento de Estado. Foi co-autor de vários relatórios RAND, inclusive: The Nuclear Asymptote: On Containing Nuclear Proliferation e The Day After... Study.